Development of a Guidebook in Support of the NASA R&M Standard

Jeffery Nunes, Jet Propulsion Laboratory, California Institute of Technology
Chester J. Everline, Jet Propulsion Laboratory, California Institute of Technology
Todd Paulos, PhD, Jet Propulsion Laboratory, California Institute of Technology
Anthony DiVenti, NASA Headquarters

Key Words: guidebook, maintainability, NASA-STD-8729.1, reliability

SUMMARY

This paper describes a guidebook currently in development to support the application of the NASA R&M Standard [1]. NASA-STD-8729.1A identifies the objectives and strategies for how to develop a system or design that is reliable and maintainable. Rather than requiring a checklist of mandatory tasks, such as specific design or Reliability & Maintainability (R&M) analyses, the standard explains objectives that need to be accomplished, and how to accomplish the objectives in the form of strategies. Currently, the standard presents the hierarchy without defining or explaining elements, or how to use the hierarchy efficiently. This is where this accompanying guideline comes into play; the guideline helps clarify through discussion and examples the standard in more detail, and how to apply it in real world situations that engineers face every day.

1 RELIABILITY, MAINTAINABILITY AND RISK

There is a relationship between reliability and maintainability (R&M) and risk. As defined in NASA-STD-8729.1A [1], reliability is the measure of the probability that an item will perform its intended function for a specified interval under stated conditions. NASA NPR-8000.4B [2] summarizes risk conceptually as follows: "in the context of mission execution, risk is the potential for performance shortfalls, which may be realized in the future, with respect to achieving explicitly established and stated performance requirements." When the performance shortfalls of risk relate to technical performance, risk and reliability are related. Specifically, an inverse relationship exists between reliability and risk, where reducing risk increases reliability and the inverse.

For maintainability, NASA-STD-8729.1A includes the following: "One expression of maintainability is the probability that an item will be retained in or restored to a specified condition within a given period of time, when the maintenance is performed in accordance with prescribed procedures and resources." Aspects of cost and schedule, as well as technical performance, are explicit in the NASA-STD-8729.1A treatment of maintainability.

Given the relationship between risk and R&M, risk provides valuable insights that can be used to guide the design, help formulate requirements, and make a system more inherently reliable and maintainable. In engineering practice, risk management is an important tool for decision making. Risk concepts and risk assessments are used to inform decision making to help balance the engineering effort and focus resources based upon the risk drivers, as explained in NPR 8000.4B for the NASA Risk Management Process and Requirements.

In the R&M hierarchy, the objectives and strategies concepts are strongly related to concepts of risk reduction. Given this relationship, discussion of the strategies for reliability and maintainability include explicit references to how they relate to risk reduction. Strategies that focus on reducing the consequences of a scenario (such as designing for fault tolerance) are referred to as mitigations. Strategies that focus on reducing the likelihood of a scenario (such as defect preventions) are referred to as preventions (preventive measures, fault avoidance).

Regardless of the primary focus of a given strategy, remedies for problems discovered in any design or testing strategy may use combinations of prevention or mitigation techniques to reduce risk and improve reliability. Because of the synergism between R&M and risk management, the R&M hierarchy should be used together with risk management processes such as the Risk Informed Decision Making (RIDM), and Continuous Risk Management (CRM) in the NASA Risk Management Process and Requirements to be effective. Refer to Ref. 2 for elaboration.

2 THE R&M HIERARCHY

The hierarchy identifies basic objectives and strategies but does not presently illustrate the process views or temporal nature of various tasks and activities. Activities and tasks need to be performed iteratively, with rigorous engineering practices, as the designs evolve and mature. This process ensures that any products or information generated remain current with the evolution of the system design. Planning activities and tasks takes into account not only the objectives, but also the timeline for when task results are needed in the product lifecycle, allowing adequate time to change the design, testing, or operations based on feedback from completed tasks. Tasks that

are performed too late reduce improvement opportunities, drive up costs, and ultimately increase technical and programmatic risk. Hence it is more appropriate that the hierarchy be used during early phases of the lifecycle (i.e., Pre-Phase A or Phase A), not only to analyze the design, but more importantly to help formulate the R&M requirements.

In addition to conventional R&M processes, interdependent related processes should be remembered, such as Verification & Validation (V&V) and Risk Management. The V&V process provides objective evidence that a system or design meets requirements and is adequate for the intended mission. Reliability products used for V&V are referred to as examples in some instances, but the hierarchy emphasizes the objectives and strategies behind these products.

2.1 R&M Hierarchy Concepts and Relationships

The layout of the hierarchy can be seen in Figure 1. Objectives describe necessary characteristics or attributes about the system or design that we are trying to accomplish. The Top Objective is the highest-level goal. It is the starting point and defines the scope of what is contained within the hierarchy. Subordinate objectives are deduced from parent strategy and objectives. Strategy describes ways or methods to accomplish the parent objective/sub-objective. The ways and methods relate to engineering practices, activities, and tasks.

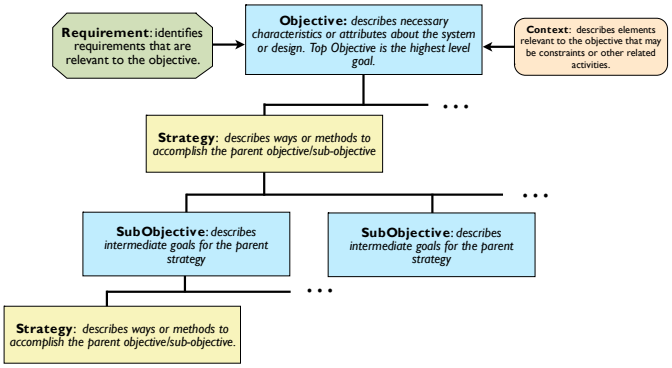

Figure 1 – R&M Hierarchy Concepts and Relationships

When considering the strategies, keep in mind the parent objective to ensure the activities and tasks developed for the strategy are consistent with and will in fact accomplish the objective. Analyses are common verification tasks that provide objective evidence that a strategy for a design or system meets is requirements. If an analysis demonstrates that a design or system meets its requirements, then the objective has been achieved.

2.2 Top Tier Objective, Strategy and Inputs

In the interest of brevity, the entire R&M hierarchy will not be presented, but only discussed as it fits into the examples of this paper; the entire hierarchy is available for review in Ref. 1. All figures describing the hierarchy are from Ref. 1. As shown in Figure 2, the top objective of the R&M Hierarchy is that the system performs as required over the lifetime to satisfy the mission requirements. The top strategy is to prevent faults and failures, provide mitigation capabilities, as needed to maintain an acceptable level of functionality considering safety, performance, and sustainability objectives.

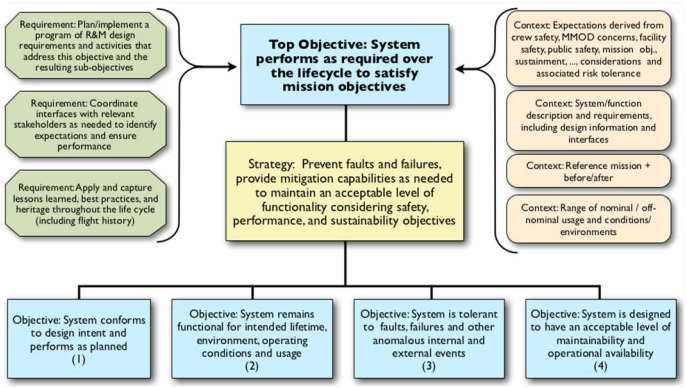

Figure 2 – R&M Structure Top Tier

The top objective articulates attributes and characteristics of a reliable system. If the criteria in the top objective is met, then a system is deemed "reliable" for the intended application. In practice, there is always uncertainty about the reliability of a system/design since success cannot be guaranteed. Therefore, a system/design is considered reliable enough when the risk is considered acceptable. The parameters of this objective (the mission, the requirements, etc.) are provided as inputs to the hierarchy shown in Requirements and Context boxes.

The top strategy summarizes the means or approach to accomplish the top objective. At the core, the strategy uses the basic concepts of risk reduction, that is (1) to consider preventive measures to reduce the likelihood of faults and failure and (2) to consider mitigations to reduce the consequences of any lower level faults or failures that may occur. These approaches are tailored to the level of acceptability determined by the requirements and contexts (the application, usage, risk posture, resources, etc.).

2.3 Top Level Requirements

There are three top level requirements that need consideration.

- Plan/Implement a program of R&M design requirements and activities that address this objective and the resulting sub-objectives

This requirement identifies that an organizational framework is needed in order to be able to implement the R&M activities. As an engineering discipline, R&M must have formal engineering structure, which includes all of the technical and programmatic management necessary to make the objective hierarchy happen.

- Coordinate interfaces with relevant stakeholders as needed to identify expectations and ensure performance

This requirement identifies that the efforts are to be coordinated and that communication is needed for the results to be effective. There are many participants in the development of the designs and systems, and much of the information used in the hierarchy comes from outside the discipline and hierarchy, such as the mission objectives, usage, environments, requirements, basic design, etc. Information must flow not only from the outside into the hierarchy, but also from the hierarchy back to the rest of the project. This helps the RIDM process and enhances the effectiveness of the work produced thru the hierarchy.

- Apply and capture lessons learned, best practices, and heritage through the life cycle, including flight history

This requirement deals with the fact that heuristic based processes and techniques learned from experience are necessary inputs to improve designs and reduce risk. Various processes and practices exist to help capture lessons learned and to develop best engineering practices. These processes are not part of the hierarchy but are important inputs to the hierarchy. This includes all previous flight history as well as design and development experience.

2.4 Top Level Context

- Expectations derived from crew safety, Micro-Meteoroid Orbital Debris (MMOD) concerns, facilities safety, public safety, mission objectives, sustainment considerations and associated risk tolerance

This input deals with the fact that design targets are derived from expectations and concerns around mission objectives, risk concerns, and other sources that must be considered in the activities from the R&M hierarchy. Although these are not developed within the hierarchy, they must be considered and the results of the R&M activities must be responsive to those expectations for the mission to be successful.

- System/Function description and requirements including design information and interfaces.

This input identifies the fact that requirements and designs established for the mission are inputs to the R&M hierarchy objectives and tasks. The set of information refers to requirements and design information that are not directly developed by the activities and tasks in the hierarchy. The tasks performed in the hierarchy use the mission/system requirements, design, and interfaces, as inputs.

- Reference mission

Many of the R&M tasks and analyses revolve around and depend upon understanding the mission and how it is supposed to happen. In practice the mission plan and details evolve over time and updates must be incorporated so the tasks results remain current for the intended mission. Hierarchy tasks also can influence the mission in various ways at different levels.

- Range of nominal/off-nominal usage and conditions/environments.

This input identifies the fact that the usage and conditions, including environments, established for the mission are inputs to the R&M hierarchy objectives and tasks.

3 SAMPLE APPLICATIONS OF THE R&M HIERARCHY

The section illustrates how NASA's R&M standard could be applied to projects within the context of NASA's overall risk management requirements and guidance. Primarily, the focus is on applying the standard in a manner consistent with the graded approach to risk management imposed by Ref. 2, and described in Refs. 3 through 5. Central to these synopses of project risks is the common 5×5 matrix. This is certainly not the only graphic available for viewing risks, and in some instances other views are more informative. However, the 5×5 matrix has broad familiarity.

Risk management includes establishing risk thresholds, goals, and applying the concept of "As Safe As Reasonably Practicable" (ASARP) expounded in Refs. 4 and 5. With respect to the 5×5 matrices used in those examples:

- high (red) risks do not meet threshold requirements;
- medium (yellow) risks are managed using the ASARP concept; and
- low (green) risks satisfy project risk goals.

The two examples discuss a payload mission that must make selective redundancy decisions, and a CubeSat mission early in the project cycle. The guidebook includes further examples of addressing risks that arise during design development, including planning an R&M program at the start of the project.

3.1 Selective Redundancy for a NASA Payload Mission

Figure 3 shows the risk profile for an Earth science instrument. The medium risks appearing in Figure 3 are defined in Table 1 in priority order; green risks are not discussed further, however they are continually tracked throughout the development cycle to ensure they stay green.

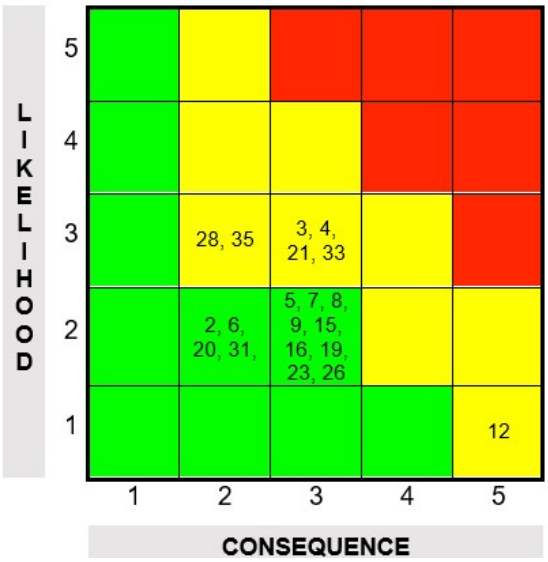

Figure 3 – Risk Matrix of Earth Science Instrument

Five of the risks (4, 21, 28, 33, and 35) result from the mission involving multiple partners (including international partners who manage the overall mission). These risks are not amenable to management using the R&M standard. Two risks, however (3 and 12), are amenable to management using the standard. Of these, Risk 12, represents a common challenge to all NASA missions, especially those with lower payload risk classifications.

Applying the R&M standard to decisions related to selective redundancy requires understanding how selective redundancy impacts risk at the system level. If p is the probability a single hardware item or string fails to perform its intended function, then the probability two independent hardware items or strings both fail to perform is on the order of p^2. Since failure probabilities tend to be small, reducing the failure probability from p to p^2 seems to afford an appreciable reliability improvement. Adding redundancy to achieve fault tolerance is only one technique for improving reliability.

Increasing the reliability of a single-string design can be achieved by reducing the likelihood of lower-level failures, such as purchasing more reliable components, derating components, testing components prior to integration, and

developing robust designs which are tolerant of hardware degradation or anomalies. None of these is universally applicable, and all entail greater cost.

Risk	Definition
3	High voltage power supply development risk
4	Instrument development schedule risk due to multiple project partners
12	Selective redundancy
21	Delayed LV selection
28	Interfacing with spacecraft due to multiple project partners
33	Assembly, Test and Launch Operations (ATLO) scheduling due to multiple project partners
35	Late selection of spacecraft bus voltage

Table 1 – Medium Risk (Yellow) Definitions for Earth Science Instrument

Implementing redundancy to achieve fault tolerance also has adverse consequences. Software is usually needed to manage the redundant strings, and additional hardware may be required for switching or other functions. The redundant hardware increases overall mass, not only because of the redundant components, but also because of wiring harnesses and any additional hardware needed to manage the redundancy (e.g., for switching). Integration can become more challenging and the added system complexity can exponentially increase testing requirements. These options also have the potential to adversely impact implementation costs and schedule.

For the science objectives, the risk is that if a single-string design (i.e., a design which is not fault tolerant) fails to function during the mission, the spacecraft will not be able to satisfy its science requirements. With respect to implementation cost and schedule risks, given that a redundant hardware item is installed to achieve fault tolerance, there is the possibility that the resultant erosion of mass or power margins, the added complexity associated with integration and testing, or the cost of the redundant hardware, harnesses, and support could adversely impact schedule and costs.

Rather than assessing the science risks of redundancy alternatives, along with the associated cost and schedule risks, the instrument project could opt to mitigate Risk 12 using a somewhat different approach. Consider a project that has robust cost and schedule reserves when this risk is identified. When the selective redundancy study begins, the project can establish cost and schedule targets which permits them to apply the ASARP process with the objective of selecting that set of redundancy alternatives which afford the greatest risk reduction, and does not exceed cost or schedule targets. Projects that identify this risk later would have fewer options available.

As for Risk 12, inspection of the R&M hierarchy (Figure 2) offers Sub-Objective 3 as most relevant for the risk stated above, the "system is tolerant to faults, failures and other anomalous internal and external events." Further expansion of the hierarchy from NASA-STD-8729.1A is shown in Figure 4. In Figure 4, that Sub-Objective (3), Strategy 3.A also applies, e.g., "assure that the system includes necessary barriers and mitigations to keep anomalous events from compromising the ability to meet the mission objectives." In the design phase of the project, the focus would be on achieving Sub-Objective 3.A.1, "System has multiple means of accomplishing functions that are critical to mission objectives, including safety." Hence, Strategy 3.A.1.A, "provide similar or dissimilar functional redundancy" is the means to accomplish this objective.

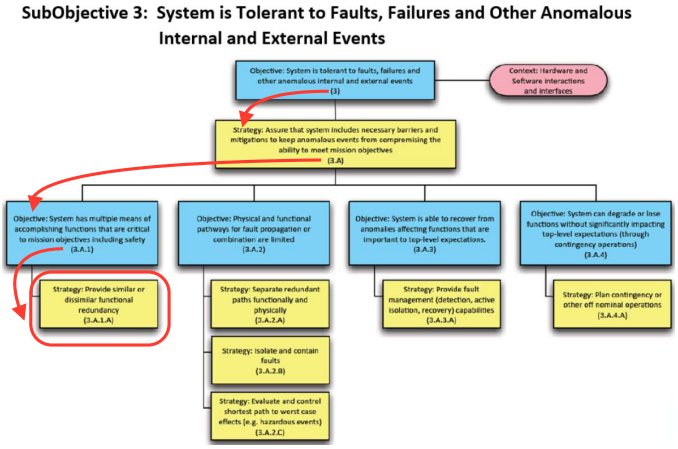

Figure 4 – Strategy 3.A.1.A Application for Selecting Redundancy

3.2 CubeSat Mission in Early Design Phase

As stated previously, missions in the early stages of design, such as Pre-Phase A or Phase A, are more amenable to mission and design changes than those in later phases of development. Analysis is typically cheaper than throwing out hardware, and there is no better time than early in the mission design to begin to identify, track and manage risks to help with the design. One admonition is that projects in early stages may have a set of risks that are less specific, even qualitative in nature, and risks levels may change over time as the design progresses, information is gained, and project resource decisions are made.

In this example, consider an earth-orbiting CubeSat mission. This mission is a technology development mission for additive manufacturing that will fly an instrument in a CubeSat form factor. Figure 5 shows the risk profile for the mission, and Table 2 defines each risk listed in priority order. This particular mission has a short duration, with relatively benign environments in terms of radiation, temperatures, and typical launch environments for instruments. There are the typical challenges due to limited resources (cost and schedule), which drive the technical and performance risk. Resource limitations also preclude a more comprehensive reliability program. Although it is a given that new technology developments carry greater risk, the question is how to use the limited resources best to improve the reliability enough to satisfy the expectations and Level 1 (L1) Requirements for the mission.

Basic expectations for this mission are as follows:

- Systems are expected to function correctly and survive the anticipated environments to satisfy L1 requirements.
- Safety and compatibility with other flight equipment that it may interface with are still required.
- Single point failures are acceptable if the failure likelihood of the single-string design is acceptably low.

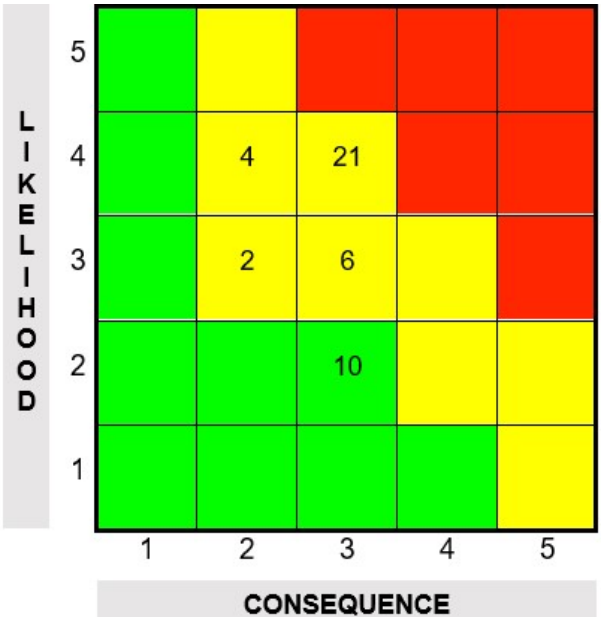

Figure 5 – Risk Matrix of CubeSat Mission Early in Design

Risk	Definition
21	Aggressive development schedule
4	Insufficient processor capabilities
6	Additive manufactured parts do not pass qualification tests
2	Electronic part availability
10	Test as you fly exception

Table 2 –Risk Definitions for CubeSat Mission Early in Design

Risks are threats to requirements. Given that the CubeSat mission is early in its lifecycle (Pre-Phase A or Phase A), the risks in Figure 5 relate directly to high-level requirements. If, the CubeSat was still a study, one risk mitigation strategy would be to negotiate with the acquirer and attempt to revise what they consider baseline and threshold risks. For example, Risk 6 implies a high-level reliability requirement for additive manufactured parts. This risk results from a requirement to demonstrate the capability of additive manufacturing. The requirement relates to baseline instead of threshold mission success, which is why the consequence level is 3. One negotiating strategy for reducing the likelihood of this risk is to limit the application of additive manufacturing to less complex shapes or less critical hardware. Since this will diminish the challenge or reduce mission sensitivity to faults of these reduce mission sensitivity to faults resulting from undetected additive manufacturing errors, the likelihood of Risk 6 should decrease. If the acquirer is not amenable to revising the requirement, techniques for managing this risk using the R&M standard would then be utilized, as describe later.

Risk 21 is a schedule risk, and not directly amenable to the NASA standard, as are other types of risk.

Addressing Risk 4 should involve the RIDM process. Since the mission is Pre-Phase A or Phase A, with respect to the R&M standard the appropriate approach is to impose reliability process requirements (i.e., perform certain analyses to inform decision-makers about the risks associated with architecting alternatives) that will be performed at an appropriate time in the overall project schedule. Certain high-level analyses can be performed now, but as the project progresses, more detailed analyses and tests to ensure that this risk has been appropriately reduced should be imposed as requirements. This same recommendation applies to Risk 2, which pertains to the use of commercial off-the-shelf (COTS) parts.

Risk 10 is currently low (i.e., satisfy project risk goals), but in a CRM context it should be monitored through development.

With respect to Risk 6, additive manufacturing is relatively new to aerospace, and no matter what the application, there is always the question of how good the printed parts are in comparison to traditionally manufactured parts. The heat printing of complex parts leaves many questions that are difficult to answer through analysis. By inspecting the objectives hierarchy, Objective (1) "system conforms to the design intent", and Objective (2) "System remains functional for the intended lifetime, environment, operating conditions, and usage" are most relevant to the reliability risk concerns. These are called out in Figure 6. Objective (3) may also apply to a lesser extent, but it is felt that Objectives (1) and (2) are more important for this particular situation.

In the interest of brevity, only Objective (1) "system conforms to the design intent" will be further expanded, although and Objective (2) is expanded in the guidebook as well: "System remains functional for the intended lifetime, environment, operating conditions, and usage" are most relevant to the reliability risk concerns. For Objective 1, refer to Figure 7.

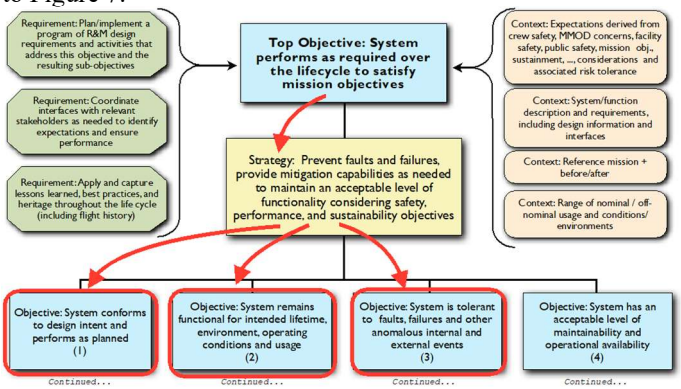

Figure 6 – Top Objective for R&M Program Planning

For Objective 1, the best path is shown in Figure 7, which leads us to Strategy 1.C "Achieve high level of process reliability"; followed by Objective 1.C.1 "Built system and its components do not contain flaws/faults that reduce the ability to withstand loads and stresses"; followed by Strategy 1.C.1.A ("Select appropriate quality components and materials") and Strategy 1.C.1.D ("Screening, proof testing and acceptance testing").

Materials used in additive manufacturing have less heritage than common aerospace materials and require additional margins. Considerations with respect to screening criteria, proof and acceptance testing need to be aspects of the RIDM process. The comparison between the reliability of the new technology and that of the technology with greater heritage and less uncertainty is not the sole consideration. This has to be

traded against other factors such as the comparison between cost, weight, performance, and schedule of these options.

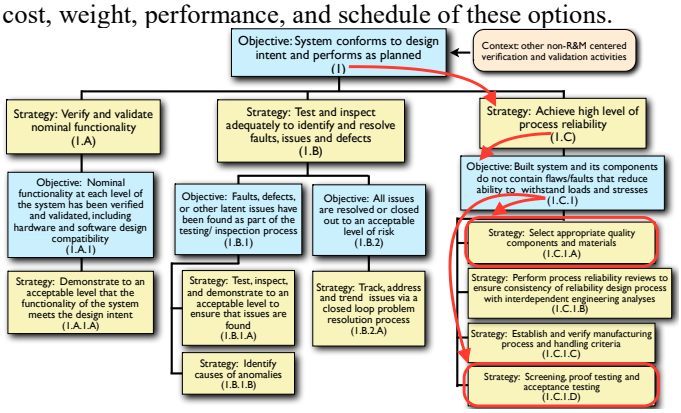

Figure 7- Objective 1 For Additive Manufacturing Risks

In addition to discussing the risks in the 5x5, the guidebook also describes how to use the hierarchy to plan the basic R&M program for this mission early in the design cycle.

4 CONCLUSION

As outlined in this paper, the NASA R&M Guidebook demonstrates with actual missions as textbook case studies how the NASA R&M Objectives Hierarchy can be used to manage risk, improve reliability and maintainability, and plan an R&M program for aerospace applications. For further clarification, consult the R&M Guidebook when completed and published.

ACKNOWLEDGEMENT

The research was carried out at the Jet Propulsion Laboratory, California Institute of Technology, under a contract with the National Aeronautics and Space Administration.

REFERENCES

1. *NASA Reliability and Maintainability (R&M) Standard for Spaceflight and Support Systems*, Draft 1, NASA-STD-8729.1A, April 25, 2015..
2. *Agency Risk Management Procedural Requirements*, NPR 8000.4B, December 6, 2017
3. H. Dezfuli, et al., *NASA Risk Management Handbook*, NASA/SP-2011-3422, Version 1.0, November 2011.
4. H. Dezfuli, et al., NASA System Safety Handbook Volume 1, System Safety Framework and Concepts for Implementation, NASA/SP-2010-580, November 2011.
5. H. Dezfuli, et al., NASA System Safety Handbook Volume 2: System Safety Concepts, Guidelines, and Implementation Examples, NASA/SP-2014-612, November 2014.

BIOGRAPHIES

Jeffery Nunes
Jet Propulsion Laboratory
California Institute of Technology
4800 Oak Grove Drive
Pasadena, CA 91109

Email: jeffery.nunes@jpl.nasa.gov

Jeffery Nunes is a principal systems engineer at Jet Propulsion Laboratory, serving as the system reliability technical lead for JPL. He has 33 years of experience in Reliability Engineering at JPL, represents JPL on the NASA R&M Technical Discipline Team, and contributed to the development of the NASA R&M Objectives Hierarchy and NASA-STD-8729.1A.

Chester J. Everline
Jet Propulsion Laboratory
California Institute of Technology
4800 Oak Grove Drive
Pasadena, CA 91109

Email: chester.j.everline@jpl.nasa.gov

Chester Everline is a principal systems engineer at the Jet Propulsion Laboratory, currently serving as the laboratory's point of contact for probabilistic risk assessment (PRA). He has over 30 years experience performing and managing PRAs in the nuclear and aerospace industries. He is a principal contributor to NASA's PRA Procedures Guide (NASA/SP-2011-3421) and a member of the NASA System Safety Steering Group. His current interest is in developing model-based mission assurance techniques to support JPL's integrated model-centric engineering efforts and the Europa Clipper Project.

Todd Paulos, PhD
Jet Propulsion Laboratory
California Institute of Technology
4800 Oak Grove Drive
Pasadena, CA 91109

Email: tpaulos@jpl.nasa.gov

Todd Paulos is a systems engineer at the Jet Propulsion Laboratory, with over 20 years experience in PRA and R&M. He is a principal contributor to NASA's PRA Procedures Guide (NASA/SP-2011-3421). His current interest is in developing risk assessment models for sample return missions.

Anthony DiVenti
NASA Headquarters
300 E St SW
Washington, DC 20546

Email: anthony.j.diventi@nasa.gov

Anthony (Tony) DiVenti is the Reliability and Maintainability (R&M) technical fellow at NASA Headquarters, where he is responsible for leading R&M policy development and providing facilitation, integration and/or oversight of R&M related research and process improvement activities. He has over 25 years of experience in the R&M, quality assurance, and systems engineering.. His current interest is to improve the state-of-the-art of R&M practices to keep pace with rapidly evolving space systems and component technologies.